

**UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION**

Andrew Willoughby, individually and on
behalf of all others similarly situated,

Plaintiff,

v.

Capital One Financial Corporation, Capital
One, N.A., and Capital One Bank (USA),
N.A.,

Defendants.

Case No.: 1:25-cv-302

JURY TRIAL DEMANDED

CLASS ACTION COMPLAINT

Plaintiff Andrew Willoughby, individually and on behalf of all others similarly situated, for his Class Action Complaint, brings this action against Defendants Capital One Financial Corporation, Capital One, N.A., and Capital One Bank (USA), N.A. (collectively, “Defendants”) based on personal knowledge and the investigation of counsel and alleges as follows:

I. INTRODUCTION

1. Between August 11, 2022 through May 22, 2023 a (now former) employee of Defendants gained access to Defendants’ inadequately protected computer systems. As a result, Plaintiff and the Class Members (as further defined below) have had their personal identifiable information (“PII”),¹ including their names, Social Security numbers, addresses, email addresses, dates of birth, telephone numbers, credit card numbers, transaction history, and other financial information exposed (the “Data Breach”).

¹ Personal identifiable information generally incorporates information that can be used to distinguish or trace an individual’s identity, either alone or when combined with other personal or identifying information. 2 C.F.R. § 200.79. At a minimum, it includes all information that on its face expressly identifies an individual.

2. Plaintiff and members of the Class were or are customers of Defendants.

3. In carrying out its business, Defendants obtains, collects, uses, and derives a benefit from the PII of Plaintiff and the Class. As such, Defendants assumed the legal and equitable duties to those individuals to protect and safeguard that information from unauthorized access and intrusion.

4. Due to Defendants' negligence, cybercriminals obtained everything they need to commit identity theft and wreak havoc on the financial and personal lives of thousands of individuals.

5. This class action seeks to redress Defendants' unlawful, willful and wanton failure to protect the personal identifiable information of thousands of individuals that was exposed in a major data breach of Defendants' network in violation of its legal obligations.

6. For the rest of their lives, Plaintiff and the Class Members will have to deal with the danger of identity thieves possessing and misusing their PII. Plaintiff and Class Members will have to spend time responding to the Breach and are at an immediate, imminent, and heightened risk of all manners of identity theft as a direct and proximate result of the Data Breach. Plaintiff and Class Members have incurred and/or will continue to incur damages in the form of, among other things, identity theft, attempted identity theft, lost time and expenses mitigating harms, increased risk of harm, damaged credit, deprivation of the value of their PII, loss of privacy, and/or additional damages as described below.

7. Defendants betrayed the trust of Plaintiff and the other Class Members by failing to properly safeguard and protect their personal identifiable information and thereby enabling cybercriminals to steal such valuable and sensitive information.

8. Plaintiff brings this action individually and on behalf of the Class, seeking remedies including, but not limited to, compensatory damages, reimbursement of out-of-pocket costs, injunctive relief, reasonable attorney fees and costs, and all other remedies this Court deems proper.

II. THE PARTIES

9. Plaintiff Andrew Willoughby is a citizen of New York.

10. Defendant Capital One Financial Corporation is a bank holding company that specializes in credit cards, auto loans, and banking and savings accounts. It is headquartered in McLean, Virginia and incorporated under the laws of the State of Delaware.

11. Defendant Capital One, N.A. is a national bank with its principal place of business in McLean, Virginia. Defendant Capital One, N.A., is a wholly owned subsidiary of Capital One Financial Corporation.

12. Defendant Capital One Bank (USA), N.A. is a national bank with its principal place of business in McLean, Virginia. Defendant Capital One Bank (USA), N.A. is a wholly owned subsidiary of Capital One Financial Corporation.

13. The true names and capacities of persons or entities, whether individual, corporate, associate, or otherwise, who may be responsible for some of the claims alleged herein are currently unknown to Plaintiff. Plaintiff will seek leave of court to amend this Complaint to reflect the true names and capacities of such other responsible parties when their identities become known.

14. All of Plaintiff's claims stated herein are asserted against Defendants and any of its owners, predecessors, successors, subsidiaries, agents and/or assigns.

III. JURISDICTION AND VENUE

15. This Court has subject matter and diversity jurisdiction over this action under 28 U.S.C. § 1332(d) because this is a class action wherein the amount of controversy exceeds the sum or value of \$5 million, exclusive of interest and costs; there are more than 100 members in the proposed class; and at least one Class Member, including Plaintiff is a citizen of a state different from Defendants to establish minimal diversity.

16. This Court has personal jurisdiction over Defendants because it conducts substantial business in Virginia and this District and collected and/or stored the PII of Plaintiff and Class Members in this District.

17. Venue is proper in this District under 28 U.S.C. § 1391(b) because Defendants operate in this District and a substantial part of the events or omissions giving rise to Plaintiff and the Class Members' claims occurred in this District, including Defendants collecting and/or storing the PII of Plaintiff and Class Members.

IV. FACTUAL ALLEGATIONS

Background

18. Defendants required that Plaintiff and Class Members provide their PII in order to do business with Defendants.

19. Plaintiff and Class Members relied on these sophisticated Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information. Plaintiff and Class Members demand security to safeguard their PII.

20. Defendants had a duty to adopt reasonable measures to protect the PII of Plaintiff and the Class Members from involuntary disclosure to third parties.

The Data Breach

21. Between August 11, 2022, through May 22, 2023, due to Defendants' failure to maintain an adequate security system, a then-employee gained access to Defendants' systems and acquired certain files and information including Plaintiff and Class Members' PII.

22. Defendants negligently delayed in responding to the notice and did not notify Plaintiff or members of the Class of the Data Breach until January 2025 ("Notice of Data Breach").²

23. Defendants admitted in the Notice of Data Breach that an unauthorized actor accessed sensitive information about Plaintiff and Class Members.³

24. The details of the root cause of the Data Breach, the vulnerabilities exploited, and the remedial measures undertaken to ensure a breach does not occur have not been shared with regulators or Plaintiff and Class Members, who retain a vested interest in ensuring that their information remains protected.

25. The unencrypted PII of Plaintiff and Class Members may end up for sale on the dark web or simply fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiff and Class Members. Unauthorized individuals can easily access the PII of Plaintiff and Class Members.

26. Defendants were negligent and did not use reasonable security procedures and practices appropriate to the nature of the sensitive, unencrypted information it was maintaining for Plaintiff and Class Members, causing the exposure of PII for Plaintiff and Class Members.

² <https://www.mass.gov/doc/assigned-data-breach-number-29805-capital-one/download>

³ *Id.*

27. Because Defendants had a duty to protect Plaintiff's and Class Members' PII, Defendants should have known through readily available and accessible information about potential threats for the unauthorized exfiltration and misuse of such information.

28. In the years immediately preceding the Data Breach, Defendants knew or should have known that Defendants' computer systems were a target for cybersecurity attacks because warnings were readily available and accessible via the internet.

29. In October 2019, the Federal Bureau of Investigation published online an article titled "High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations" that, among other things, warned that "[a]lthough state and local governments have been particularly visible targets for ransomware attacks, ransomware actors have also targeted health care organizations, industrial companies, and the transportation sector."⁴

30. In April 2020, ZDNet reported, in an article titled "Ransomware mentioned in 1,000+ SEC filings over the past year," that "[r]ansomware gangs are now ferociously aggressive in their pursuit of big companies. They breach networks, use specialized tools to maximize damage, leak corporate information on dark web portals, and even tip journalists to generate negative news for companies as revenge against those who refuse to pay."⁵

31. In September 2020, the United States Cybersecurity and Infrastructure Security Agency published online a "Ransomware Guide" advising that "[m]alicious actors have adjusted their ransomware tactics over time to include pressuring victims for payment by threatening to

⁴ FBI, High-Impact Ransomware Attacks Threaten U.S. Businesses and Organizations (Oct. 2, 2019) (emphasis added), *available at* <https://www.ic3.gov/Media/Y2019/PSA191002> (last visited Jan. 25, 2022).

⁵ ZDNet, Ransomware mentioned in 1,000+ SEC filings over the past year (Apr. 30, 2020) (emphasis added), *available at* <https://www.zdnet.com/article/ransomware-mentioned-in-1000-sec-filings-over-the-past-year/> (last visited Jan. 25, 2022).

release stolen data if they refuse to pay and publicly naming and shaming victims as secondary forms of extortion.”⁶

32. This readily available and accessible information confirms that, prior to the Data Breach, Defendants knew or should have known that: (i) cybercriminals were targeting big companies such as Defendants, (ii) cybercriminals were ferociously aggressive in their pursuit of companies in possession of significant sensitive information such as Defendants, (iii) cybercriminals were leaking corporate information on dark web portals, and (iv) cybercriminals’ tactics included threatening to release stolen data.

33. Considering the information readily available and accessible on the internet before the Data Breach, Defendants, having elected to store the unencrypted PII of Plaintiff and Class Members in an Internet-accessible environment, had reason to be on guard for the exfiltration of the PII, and Defendants’ type of business had cause to be particularly on guard against such an attack.

34. Prior to the Data Breach, Defendants knew or should have known that there was a foreseeable risk that Plaintiff’s and Class Members’ PII could be accessed, exfiltrated, and published as the result of a cyberattack.

35. Prior to the Data Breach, Defendants knew or should have known that it should have encrypted the Social Security numbers and other sensitive data elements within the PII to protect against their publication and misuse in the event of a cyberattack.

Defendants Acquires, Collects, and Stores the PII of Plaintiff and Class Members

36. Defendants acquired, collected, and stored the PII of Plaintiff and Class Members.

⁶ U.S. CISA, Ransomware Guide – September 2020, available at https://www.cisa.gov/sites/default/files/publications/CISA_MS-ISAC_Ransomware%20Guide_S508C.pdf (last visited Jan. 25, 2022).

37. Plaintiff and other members of the Class entrusted their PII to Defendants.

38. By obtaining, collecting, and storing the PII of Plaintiff and Class Members, Defendants assumed legal and equitable duties and knew or should have known that it was responsible for protecting the PII from disclosure.

39. Plaintiff and Class Members have taken reasonable steps to maintain the confidentiality of their PII and relied on Defendants to keep their PII confidential and securely maintained, to use this information for business purposes only, and to make only authorized disclosures of this information.

40. As explained by the Federal Bureau of Investigation, “[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection.”⁷

41. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Government, the following measures:

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.
- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.
- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.
- Configure firewalls to block access to known malicious IP addresses.

⁷ See How to Protect Your Networks from RANSOMWARE, at 3, available at <https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view> (last visited July 17, 2023).

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.
- Set anti-virus and anti-malware programs to conduct regular scans automatically.
- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment.
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.⁸

42. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the United States Cybersecurity & Infrastructure Security Agency, the following measures:

⁸ *Id.* at 3-4.

- **Update and patch your computer.** Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks. . . .
- **Use caution with links and when entering website addresses.** Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net). . . .
- **Open email attachments with caution.** Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.
- **Keep your personal information safe.** Check a website's security to ensure the information you submit is encrypted before you provide it. . . .
- **Verify email senders.** If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.
- **Inform yourself.** Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques. You can find information about known phishing attacks on the Anti-Phishing Working Group website. You may also want to sign up for CISA product notifications, which will alert you when a new Alert, Analysis Report, Bulletin, Current Activity, or Tip has been published.
- **Use and maintain preventative software programs.** Install antivirus software, firewalls, and email filters—and keep them updated—to reduce malicious network traffic. . . .⁹

⁹ See Security Tip (ST19-001) Protecting Against Ransomware (original release date Apr. 11, 2019), *available at* <https://www.cisa.gov/news-events/news/protecting-against-ransomware> (last visited July 17, 2023).

43. To prevent and detect ransomware attacks, including the ransomware attack that resulted in the Data Breach, Defendants could and should have implemented, as recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

Secure internet-facing assets

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; Remove privilege credentials

Thoroughly investigate and remediate alerts

- Prioritize and treat commodity malware infections as potential full compromise

Include IT Pros in security discussions

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely

Build credential hygiene

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords
- Apply principle of least-privilege

Monitor for adversarial activities

- Hunt for brute force attempts
- Monitor for cleanup of Event logs
- Analyze logon events

Harden infrastructure

- Use Windows Defender Firewall
- Enable tamper protection
- Enable cloud-delivered protection
- Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].¹⁰

44. Given that Defendants were storing the PII of other individuals, Defendants could and should have implemented all of the above measures to prevent and detect ransomware attacks.

¹⁰ See Human-operated ransomware attacks: A preventable disaster (Mar 5, 2020), *available at* <https://www.microsoft.com/security/blog/2020/03/05/human-operated-ransomware-attacks-a-preventable-disaster/> (last visited July 17, 2023).

45. The occurrence of the Data Breach indicates that Defendants failed to adequately implement one or more of the above measures to prevent ransomware attacks, resulting in the Data Breach and the exposure of the PII of Plaintiff and Class Members.

Securing PII and Preventing Breaches

46. Defendants could have prevented this Data Breach by properly securing and encrypting the folders, files, and or data fields containing the PII of Plaintiff and Class Members. Alternatively, Defendants could have destroyed the data it no longer had a reasonable need to maintain or only stored data in an Internet-accessible environment when there was a reasonable need to do so.

47. Defendants' negligence in safeguarding the PII of Plaintiff and Class Members is exacerbated by the repeated warnings and alerts directed to protecting and securing sensitive data.

48. Despite the prevalence of public announcements of data breach and data security compromises, Defendants failed to take appropriate steps to protect the PII of Plaintiff and Class Members from being compromised.

49. The ramifications of Defendants' failure to keep secure the PII of Plaintiff and Class Members are long lasting and severe. Once PII is stolen, particularly Social Security numbers, fraudulent use of that information and damage to victims may continue for years.

Defendants' Response to the Data Breach is Inadequate

50. Defendants were negligent and failed to inform Plaintiff and the Class Members of the Data Breach in time for them to protect themselves from identity theft.

51. The Data Breach occurred in August 2022. Yet, Defendants did not start notifying affected individuals until January 2025.

52. During these intervals, the cybercriminals have had the opportunity to exploit the Plaintiff and the Class Member's PII.

Value of PII

53. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials. For example, personal information can be sold at a price ranging from \$40 to \$200, and bank details have a price range of \$50 to \$200.¹¹ Experian reports that a stolen credit or debit card number can sell for \$5 to \$110 on the dark web.¹² Criminals can also purchase access to entire company data breaches from \$900 to \$4,500.¹³

54. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach because, there, victims can cancel or close credit and debit card accounts. The information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

55. This data demands a much higher price on the black market. Martin Walter, senior director at cybersecurity firm RedSeal, explained, "Compared to credit card information,

¹¹ *Your personal data is for sale on the dark web. Here's how much it costs*, Digital Trends, Oct. 16, 2019, available at: <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed July 17, 2023).

¹² *Here's How Much Your Personal Information Is Selling for on the Dark Web*, Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed July 17, 2023).

¹³ *In the Dark*, VPNOverview, 2019, available at: <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed July 17, 2023).

personally identifiable information and Social Security numbers are worth more than 10x on the black market.”¹⁴

56. Among other forms of fraud, identity thieves may obtain driver’s licenses, government benefits, medical services, and housing or even give false information to police.

57. One such example of criminals using PII for profit is the development of “Fullz” packages.

58. Cybercriminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals. These dossiers are known as “Fullz” packages.

59. The development of “Fullz” packages means that stolen PII from the Data Breach can easily be used to link and identify it to Plaintiff’s and the Class’ phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII stolen by the cybercriminals in the Data Breach, criminals can easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

60. That is exactly what is happening to Plaintiff and members of the Class, and it is reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s and the Class’s stolen PII is being misused, and that such misuse is fairly traceable to the Data Breach.

¹⁴ Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen Credit Card Numbers*, IT World, (Feb. 6, 2015), available at: <https://www.networkworld.com/article/2880366/anthem-hack-personal-data-stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html> (last accessed July 17, 2023).

Plaintiff's Experience

61. Plaintiff is a customer of Capital One.

62. Recently, Plaintiff experienced an unauthorized charge on his Capital One credit account.

63. As a result of the Data Breach, Plaintiff's sensitive information may have been accessed and/or acquired by an unauthorized actor. The confidentiality of Plaintiff's sensitive information has been irreparably harmed. For the rest of his life, Plaintiff will have to worry about when and how his sensitive information may be shared or used to his detriment

64. As a result of the Data Breach, Plaintiff spent time dealing with the consequences of the Data Breach, which includes times spent verifying the legitimacy of the Notice of Data Breach and self-monitoring his accounts. This time has been lost forever and cannot be recaptured.

65. Additionally, Plaintiff is very careful about not sharing his sensitive PII. He has never knowingly transmitted unencrypted sensitive PII over the internet or any other unsecured source.

66. Plaintiff stores any documents containing his sensitive PII in safe and secure locations or destroys the documents. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

67. Plaintiff suffered lost time, annoyance, interference, and inconvenience as a result of the Data Breach and experiences fear and anxiety and increased concern for the loss of his privacy.

68. Plaintiff has suffered imminent and impending injury arising from the substantially increased risk of fraud, identity theft, and misuse resulting from her PII, especially his Social Security number, being placed in the hands of unauthorized third parties and possibly criminals.

69. Plaintiff has a continuing interest in ensuring that his PII, which, upon information and belief, remains backed up in Defendants' possession, is protected and safeguarded from future breaches.

Plaintiff and the Class Face Significant Risk of Continued Identity Theft

70. Plaintiff and members of the proposed Class have suffered injury from the misuse of their PII that can be directly traced to Defendants.

71. Defendants negligently disclosed the PII of Plaintiff and the Class for criminals to use in the conduct of criminal activity. Specifically, Defendants opened up, disclosed, and exposed the PII of Plaintiff and the Class to people engaged in disruptive and unlawful business practices and tactics, including online account hacking, unauthorized use of financial accounts, and fraudulent attempts to open unauthorized financial accounts (i.e., identity fraud), all using the stolen PII.

72. As a result of Defendants' negligence and failure to prevent the Data Breach, Plaintiff and the Class have suffered and will continue to suffer damages, including monetary losses, lost time, anxiety, and emotional distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their PII is used;
- b. The diminution in value of their PII;
- c. The compromise and continuing publication of their PII;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences

of the Data Breach, including, but not limited to, efforts spend researching how to prevent, detect, contest, and recover form identity theft and fraud;

- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen PII; and
- h. The continued risk to their PII, which remains in Defendants’ possession and is subject to further breaches so long as Defendants fails to undertake the appropriate measures to protect the PII in their possession.

73. The fraudulent activity resulting from the Data Breach may not come to light for years.

74. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used. According to the U.S. Government Accountability Office (“GAO”), which conducted a study regarding data breaches:

[L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.¹⁵

75. Defendants’ negligence and failure to properly notify Plaintiff and members of the Class of the Data Breach exacerbated Plaintiff’s and the Class’s injury by depriving them of the earliest ability to take appropriate measures to protect their PII and take other necessary steps to mitigate the harm caused by the Data Breach

76. Plaintiff and Class Members now face years of constant surveillance of their financial and personal records, monitoring, and loss of rights. The Classes are incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

¹⁵ *Report to Congressional Requesters*, GAO, at 29 (June 2007), available at: <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed July 17, 2023).

77. Defendants were, or should have been, fully aware of the unique type and the significant volume of data contained in Defendants' database, amounting to potentially thousands of individuals detailed, personal information and, thus, the significant number of individuals who would be harmed by the exposure of the unencrypted data.

78. At all relevant times, Defendants knew, or reasonably should have known, of the importance of safeguarding the PII of Plaintiff and Class Members, including Social Security numbers, and of the foreseeable consequences that would occur if Defendants' data security system was breached, including, specifically, the significant costs that would be imposed on Plaintiff and Class Members as a result of a breach.

79. To date, Defendants have offered Plaintiff and some Class Members only twelve (12) months of credit monitoring services. This offered service is inadequate to protect Plaintiff and Class Members from the threats they face for years to come, particularly in light of the PII at issue here.

80. The injuries to Plaintiff and Class Members are directly and proximately caused by Defendants' negligence and failure to implement or maintain adequate data security measures for the PII of Plaintiff and Class Members.

Defendants Failed to Adhere to Federal Trade Commission (FTC) Guidelines

81. According to the Federal Trade Commission ("FTC"), the need for data security should be factored into all business decision-making. To that end, the FTC has issued numerous guidelines identifying best data security practices that businesses, such as Defendants, should employ to protect against the unlawful exposure of PII.

82. The FTC defines identity theft as “a fraud committed or attempted using the identifying information of another person without authority.”¹⁶ The FTC describes “identifying information” as “any name or number that may be used, alone or in conjunction with any other information, to identify a specific person,” including, among other things, “[n]ame, Social Security number, date of birth, official State or government issued driver’s license or identification number, alien registration number, government passport number, employer or taxpayer identification number.”¹⁷

83. In 2016, the FTC updated its publication, *Protecting Personal Information: A Guide for Business*, which established guidelines for fundamental data security principles and practices for business. The guidelines explain that businesses should:

- a. Protect the sensitive consumer information that they keep;
- b. Properly dispose of PII that is no longer needed;
- c. Encrypt information stored on computer networks;
- d. Understand their network’s vulnerabilities; and
- e. Implement policies to correct security problems.

84. The guidelines also recommend that businesses watch for large amounts of data being transmitted from the system and have a response plan ready in the event of a breach.

85. The FTC recommends that companies not maintain information longer than is needed for authorization of a transaction; limit access to sensitive data; require complex passwords to be used on networks; use industry-tested methods for security; monitor for suspicious activity

¹⁶ 17 C.F.R. § 248.201 (2013).

¹⁷ *Id.*

on the network; and verify that third-party service providers have implemented reasonable security measures.

86. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act (“FTC Act”), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

87. Defendants’ negligence and failure to employ reasonable and appropriate measures to protect against unauthorized access to Plaintiff and the Class’s PII constitutes an unfair act or practice prohibited by Section 5 of the FTC Act, 15 U.S.C. § 45.

V. CLASS ACTION ALLEGATIONS

88. Plaintiff brings this nationwide class action on behalf of herself and on behalf of all others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4) of the Federal Rules of Civil Procedure.

89. The Class that Plaintiff seeks to represent is defined as follows:

All individuals whose PII may have been accessed and/or acquired in the ransomware attack that is the subject of the Notice of Data Breach that Defendants sent to Plaintiff and Class Members on or around January and February 2025 (the “Class”).

90. Excluded from the Classes are the following individuals and/or entities: Defendants and Defendants’ parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendants has a controlling interest; all individuals who make a timely election to be excluded from this proceeding using the correct protocol for opting out; any and all federal, state or local governments, including but not limited to their departments, agencies, divisions, bureaus, boards,

sections, groups, counsels and/or subdivisions; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

91. Plaintiff reserves the right to modify or amend the definition of the proposed classes before the Court determines whether certification is appropriate.

92. **Numerosity (Fed R. Civ. P. 23(a)(1)):** The Class is so numerous that joinder of all members is impracticable. Thousands of individuals had their information impacted by the Data Breach.

93. **Commonality (Fed. R. Civ. P. 23(a)(2) & (b)(3)):** Questions of law and fact common to the Classes exist and predominate over any questions affecting only individual Class Members. These include:

- a. Whether and to what extent Defendants had a duty to protect the PII of Plaintiff and Class Members;
- b. Whether Defendants had duties not to disclose the PII of Plaintiff and Class Members to unauthorized third parties;
- c. Whether Defendants had duties not to use the PII of Plaintiff and Class Members for non-business purposes;
- d. Whether Defendants failed to adequately safeguard the PII of Plaintiff and Class Members;
- e. When Defendants actually learned of the Data Breach;
- f. Whether Defendants adequately, promptly, and accurately informed Plaintiff and Class Members that their PII had been compromised;
- g. Whether Defendants violated the law by failing to promptly notify Plaintiff and Class Members that their PII had been compromised;

- h. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- i. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- j. Whether Defendants engaged in unfair, unlawful, or deceptive practice by failing to safeguard the PII of Plaintiff and Class Members;
- k. Whether Plaintiff and Class Members are entitled to actual, consequential, and/or nominal damages as a result of Defendants' wrongful conduct;
- l. Whether Plaintiff and Class Members are entitled to restitution as a result of Defendants' wrongful conduct; and
- m. Whether Plaintiff and Class Members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

94. **Typicality (Fed. R. Civ. P. 23(a)(3)):** Plaintiff's claims are typical of those of other Class Members because all had their PII compromised as a result of the Data Breach, due to Defendants' misfeasance.

95. **Policies Generally Applicable to the Class:** This class action is also appropriate for certification because Defendants have acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards of conduct toward Class Members and making final injunctive relief appropriate with respect to the Class as a whole. Defendants' policies challenged herein apply to and affect Class

Members uniformly and Plaintiff's challenge of these policies hinges on Defendants' conduct with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.

96. **Adequacy (Fed. R. Civ. P. 23(a)(4)):** Plaintiff will fairly and adequately represent and protect the interests of Class Members in that they have no disabling conflicts of interest that would be antagonistic to those of the other members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the members of the Class and the infringement of the rights and the damages they have suffered are typical of other Class Members. Plaintiff has retained counsel experienced in complex class action litigation, and Plaintiff intends to prosecute this action vigorously.

97. **Superiority and Manageability (Fed. R. Civ. P. 23(b)(3)):** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require. Class action treatment will permit the adjudication of relatively modest claims by certain Class Members, who could not individually afford to litigate a complex claim against large corporations, like Defendants. Further, even for those Class Members who could afford to litigate such a claim, it would still be economically impractical and impose a burden on the courts.

98. The nature of this action and the nature of laws available to Plaintiff and Class Members make the use of the class action device a particularly efficient and appropriate procedure to afford relief to Plaintiff and Class Members for the wrongs alleged because Defendants would necessarily gain an unconscionable advantage since it would be able to exploit and overwhelm the

limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiff was exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would create a risk of inconsistent results and would be unnecessary and duplicative of this litigation.

99. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class Members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

100. Adequate notice can be given to Class Members directly using information maintained in Defendants' records.

101. Unless a Class-wide injunction is issued, Defendants may continue in their failure to properly secure the PII of Class Members, Defendants may continue to refuse to provide proper notification to Class Members regarding the Data Breach, and Defendants may continue to act unlawfully as set forth in this Complaint.

102. Further, Defendants have acted or refused to act on grounds generally applicable to the Classes and, accordingly, final injunctive or corresponding declaratory relief with regard to Class Members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

103. Likewise, particular issues under Rule 23(c)(4) are appropriate for certification because such claims present only particular, common issues, the resolution of which would

advance the disposition of this matter and the parties' interests therein. Such particular issues include, but are not limited to:

- a. Whether Defendants owed a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- b. Whether Defendants breached a legal duty to Plaintiff and Class Members to exercise due care in collecting, storing, using, and safeguarding their PII;
- c. Whether Defendants failed to comply with their own policies and applicable laws, regulations, and industry standards relating to data security;
- d. Whether Defendants adequately and accurately informed Plaintiff and Class Members that their PII had been compromised;
- e. Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- f. Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiff and Class Members; and,
- g. Whether Class Members are entitled to actual, consequential, and/or nominal damages, and/or injunctive relief as a result of Defendants' wrongful conduct.

VI. CAUSES OF ACTION

COUNT I – NEGLIGENCE **(On Behalf of Plaintiff and the Class)**

104. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

105. Defendants solicited, gathered, and stored the PII Plaintiff and the Class as part of the operation of its business.

106. Upon accepting and storing the PII of Plaintiff and Class Members, Defendants undertook and owed a duty to Plaintiff and Class Members to exercise reasonable care to secure and safeguard that information and to use secure methods to do so.

107. Defendants had full knowledge of the sensitivity of the PII, the types of harm that Plaintiff and Class Members could and would suffer if the PII was wrongfully disclosed, and the importance of adequate security.

108. Plaintiff and Class Members were the foreseeable victims of any inadequate safety and security practices. Plaintiff and the Class Members had no ability to protect their PII that was in Defendants' possession. As such, a special relationship existed between Defendants and Plaintiff and the Class.

109. Defendants were well aware of the fact that cybercriminals routinely target large corporations through cyberattacks in an attempt to steal sensitive PII.

110. Defendants owed Plaintiff and the Class Members a common law duty to use reasonable care to avoid causing foreseeable risk of harm to Plaintiff and the Class when obtaining, storing, using, and managing personal information, including taking action to reasonably safeguard such data.

111. Defendants' duty extended to protecting Plaintiff and the Class from the risk of foreseeable criminal conduct of third parties, which has been recognized in situations where the actor's own conduct or misconduct exposes another to the risk or defeats protections put in place to guard against the risk, or where the parties are in a special relationship. *See* Restatement (Second) of Torts § 302B. Numerous courts and legislatures also have recognized the existence of a specific duty to reasonably safeguard personal information.

112. Defendants had duties to protect and safeguard the PII of Plaintiff and the Class from being vulnerable to cyberattacks by taking common-sense precautions when dealing with sensitive PII. Additional duties that Defendants owed Plaintiff and the Class include:

- a. To exercise reasonable care in designing, implementing, maintaining, monitoring, and testing Defendants' networks, systems, protocols, policies, procedures and practices to ensure that Plaintiff's and Class Members' PII was adequately secured from impermissible access, viewing, release, disclosure, and publication;
- b. To protect Plaintiff's and Class Members' PII in its possession by using reasonable and adequate security procedures and systems;
- c. To implement processes to quickly detect a data breach, security incident, or intrusion involving their networks and servers; and
- d. To promptly notify Plaintiff and Class Members of any data breach, security incident, or intrusion that affected or may have affected their PII.

113. Defendants were the only one who could ensure that its systems and protocols were sufficient to protect the PII that Plaintiff and the Class had entrusted to it.

114. Defendants breached its duties of care by failing to adequately protect Plaintiff's and Class Members' PII. Defendants breached its duties by, among other things:

- a. Failing to exercise reasonable care in obtaining, retaining securing, safeguarding, deleting, and protecting the PII in its possession;
- b. Failing to protect the PII in its possession using reasonable and adequate security procedures and systems;

- c. Failing to adequately train its employees to not store PII longer than absolutely necessary;
- d. Failing to consistently enforce security policies aimed at protecting Plaintiff's and the Class's PII; and
- e. Failing to implement processes to quickly detect data breaches, security incidents, or intrusions.

115. Defendants' willful failure to abide by these duties was wrongful, reckless, and grossly negligent in light of the foreseeable risks and known threats.

116. As a proximate and foreseeable result of Defendants' negligent and/or grossly negligent conduct, Plaintiff and the Class have suffered damages and are at imminent risk of additional harms and damages.

117. Through Defendants' acts and omissions described herein, including but not limited to Defendants' failure to protect the PII of Plaintiff and Class Members from being stolen and misused, Defendants unlawfully breached its duty to use reasonable care to adequately protect and secure the PII of Plaintiff and Class Members while it was within Defendants' possession and control.

118. As a result of the Data Breach, Plaintiff and Class Members have spent time, effort, and money to mitigate the actual and potential impact of the Data Breach on their lives, including but not limited to, closely reviewing and monitoring bank accounts, credit reports, and statements sent from providers and their insurance companies and the payment for credit monitoring and identity theft prevention services.

119. Defendants' wrongful actions, inactions, and omissions constituted (and continue to constitute) common law negligence.

120. The damages Plaintiff and the Class have suffered and will suffer were and are the direct and proximate result of Defendants' negligent and/or grossly negligent conduct.

COUNT II – NEGLIGENCE *PER SE*
(On Behalf of Plaintiff and the Class)

121. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

122. In addition to its duties under common law, Defendants had additional duties imposed by statute and regulations, including the duties the FTC Act. The harms which occurred as a result of Defendants' failure to observe these duties, including the loss of privacy and significant risk of identity theft, are the types of harm that these statutes and their regulations were intended to prevent.

123. Pursuant to the FTC Act, 15 U.S.C. § 45, Defendants had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiff and Class Members' PII.

124. Section 5 of the FTC Act prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect PII. The FTC publications and orders also form part of the basis of Defendants' duty in this regard.

125. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect consumers PII and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of PII it obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiff and Class Members.

126. Defendants' violation of Section 5 of the FTC Act constitutes negligence *per se* as Defendants' violation of the FTC Act establishes the duty and breach elements of negligence.

127. Plaintiff and Class Members are within the class of persons that the FTC Act was intended to protect.

128. The harm that occurred as a result of the Data Breach is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses, which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiff and the Class.

129. But for Defendants' wrongful and negligent breach of its duties owed to Plaintiff and Class Members, Plaintiff and Class Members would not have been injured.

130. The injury and harm suffered by Plaintiff and Class Members was the reasonably foreseeable result of Defendants' breach of its duties. Defendants knew or should have known that it was failing to meet their duties, and that Defendants' breach would cause Plaintiff and Class Members to experience the foreseeable harms associated with the exposure of their PII.

131. As a direct and proximate result of Defendants' negligent conduct, Plaintiff and Class Members have suffered injury and are entitled to compensatory, consequential, and punitive damages in an amount to be proven at trial.

COUNT III – INVASION OF PRIVACY
(On Behalf of Plaintiff and the Class)

132. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

133. Plaintiff and Class Members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

134. Defendants owed a duty to Plaintiff and Class Member to keep their PII confidential.

135. Defendants affirmatively and recklessly disclosed Plaintiff and Class Members' PII to unauthorized third parties.

136. The unauthorized disclosure and/or acquisition (i.e., theft) by a third party of Plaintiff and Class Members' PII is highly offensive to a reasonable person.

137. Defendants' reckless and negligent failure to protect Plaintiff and Class Members' PII constitutes an intentional interference with Plaintiff and the Class Members' interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

138. In failing to protect Plaintiff and Class Members' PII, Defendants acted with a knowing state of mind when it permitted the Data Breach because it knew its information security practices were inadequate.

139. Because Defendants failed to properly safeguard Plaintiff and Class Members' PII, Defendants had notice and knew that its inadequate cybersecurity practices would cause injury to Plaintiff and the Class.

140. Defendants knowingly did not notify Plaintiff and Class Members in a timely fashion about the Data Breach.

141. As a proximate result of Defendants' acts and omissions, Plaintiff and the Class Members' private and sensitive PII was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiff and the Class to suffer damages.

142. Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiff and the Class since their PII are still maintained by Defendants with their inadequate

cybersecurity system and policies.

143. Plaintiff and Class Members have no adequate remedy at law for the injuries relating to Defendants' continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendants' inability to safeguard Plaintiff and the Class's PII.

144. Plaintiff, on behalf of herself and Class Members, seeks injunctive relief to enjoin Defendants from further intruding into the privacy and confidentiality of Plaintiff and Class Members' PII.

145. Plaintiff, on behalf of herself and Class Members, seeks compensatory damages for Defendants' invasion of privacy, which includes the value of the privacy interest invaded by Defendants, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT IV – BREACH OF IMPLIED CONTRACT
(On Behalf of Plaintiff and the Class)

146. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

147. By requiring Plaintiff and the Class Members PII receive services from Defendants, Defendants entered into an implied contract in which Defendants agreed to comply with its statutory and common law duties to protect Plaintiff and Class Members' PII. In return, Defendants provided goods to Plaintiff and the Class.

148. Based on this implicit understanding, Plaintiff and the Class accepted Defendants' offers and provided Defendants with their PII.

149. Plaintiff and Class Members would not have provided their PII to Defendants had they known that Defendants would not safeguard their PII, as promised.

150. Plaintiff and Class Members fully performed their obligations under the implied contracts with Defendants.

151. Defendants breached the implied contracts by failing to safeguard Plaintiff and Class Members' PII.

152. Defendants also breached the implied contracts when it engaged in acts and/or omissions that are declared unfair trade practices by the FTC. These acts and omissions included (i) representing, either expressly or impliedly, that it would maintain adequate data privacy and security practices and procedures to safeguard the PII from unauthorized disclosures, releases, data breaches, and theft; (ii) omitting, suppressing, and concealing the material fact of the inadequacy of the privacy and security protections for the Class's PII; and (iii) failing to disclose to Plaintiff and the Class at the time they provided their PII that Defendants' data security system and protocols failed to meet applicable legal and industry standards.

153. The losses and damages Plaintiff and Class Members sustained were the direct and proximate result of Defendants' breach of the implied contract with Plaintiff and Class Members.

COUNT V – BREACH OF CONFIDENCE
(On Behalf of Plaintiff and the Class)

154. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

155. Defendants were fully aware of the confidential nature of the PII of Plaintiff and Class Members that it was provided.

156. As alleged herein and above, Defendants' relationship with Plaintiff and the Class was governed by promises and expectations that Plaintiff and Class Members' PII would be collected, stored, and protected in confidence, and would not be accessed by, acquired by,

appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

157. Plaintiff and Class Members provided their respective PII to Defendants with the explicit and implicit understandings that Defendants would protect and not permit the PII to be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties.

158. Plaintiff and Class Members provided their PII to Defendants with the explicit and implicit understandings that Defendants would take precautions to protect their PII from unauthorized access, acquisition, appropriation, disclosure, encumbrance, exfiltration, release, theft, use, and/or viewing, such as following basic principles of protecting their networks and data systems.

159. Defendants voluntarily received, in confidence, Plaintiff and Class Members' PII with the understanding that the PII would not be accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by the public or any unauthorized third parties.

160. Due to Defendants' failure to prevent, detect, and avoid the Data Breach from occurring by, inter alia, not following best information security practices to secure Plaintiff and Class Members' PII, Plaintiff and Class Members' PII was accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties beyond Plaintiff and Class Members' confidence, and without their express permission.

161. As a direct and proximate cause of Defendants' actions and/or omissions, Plaintiff and Class Members have suffered damages as alleged herein.

162. But for Defendants' failure to maintain and protect Plaintiff and Class Members' PII in violation of the parties' understanding of confidence, their PII would not have been accessed by, acquired by, appropriated by, disclosed to, encumbered by, exfiltrated by, released to, stolen by, used by, and/or viewed by unauthorized third parties. Defendants' Data Breach was the direct and legal cause of the misuse of Plaintiff and Class Members' PII, as well as the resulting damages.

163. The injury and harm Plaintiff and Class Members suffered and will continue to suffer was the reasonably foreseeable result of Defendants' unauthorized misuse of Plaintiff and Class Members' PII. Defendants knew its data systems and protocols for accepting and securing Plaintiff and Class Members' PII had security and other vulnerabilities that placed Plaintiff and Class Members' PII in jeopardy.

164. As a direct and proximate result of Defendants' breaches of confidence, Plaintiff and Class Members have suffered and will suffer injury, as alleged herein, including but not limited to (a) actual identity theft; (b) the compromise, publication, and/or theft of their PII; (c) out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft and/or unauthorized use of their PII; (d) lost opportunity costs associated with effort expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breach, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from identity theft; (e) the continued risk to their PII, which remains in Defendants' possession and is subject to further unauthorized disclosures so long as Defendants fail to undertake appropriate and adequate measures to protect Class Members' PII in their continued possession; (f) future costs in terms of time, effort, and money that will be expended as result of the Data Breach for the remainder of the lives of Plaintiff and Class Members; and (g) the diminished value of Plaintiff and Class Members' PII.

COUNT VI – BREACH OF FIDUCIARY DUTY
(On Behalf of Plaintiff and the Class)

165. Plaintiff incorporates by reference all preceding factual allegations as though fully alleged herein.

166. A relationship existed between Plaintiff and Class Members and Defendants in which Plaintiff and the Class put their trust in Defendants to protect their PII. Defendants accepted this duty and obligation when it received Plaintiff and the Class Members' PII.

167. Plaintiff and the Class Members entrusted their PII to Defendants on the premise and with the understanding that Defendants would safeguard their information, use their PII for business purposes only, and refrain from disclosing their PII to unauthorized third parties.

168. Defendants knew or should have known that the failure to exercise due care in the collecting, storing, and using of individual's PII involved an unreasonable risk of harm to Plaintiff and the Class, including harm that foreseeably could occur through the criminal acts of a third party.

169. Defendants' fiduciary duty required it to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other things, designing, maintaining, and testing Defendants' security protocols to ensure that Plaintiff and the Class's information in Defendants' possession was adequately secured and protected.

170. Defendants also had a fiduciary duty to have procedures in place to detect and prevent improper access and misuse of Plaintiff's and the Class's PII. Defendants' duty to use reasonable security measures arose as a result of the special relationship that existed between Defendants and Plaintiff and the Class. That special relationship arose because Defendants was entrusted with Plaintiff and the Class's PII.

171. Defendants breached its fiduciary duty that it owed Plaintiff and the Class by failing to case in good faith, fairness, and honesty; by failing to act with the highest and finest loyalty; and by failing to protect the PII of Plaintiff and the Class Members.

172. Defendants' breach of fiduciary duties was a legal cause of damages to Plaintiff and the Class.

173. But for Defendants' breach of fiduciary duty, the damage to Plaintiff and the Class would not have occurred, and the Data Breach contributed substantially to producing the damage to Plaintiff and the Class.

174. As a direct and proximate result of Defendants' breach of fiduciary duty, Plaintiff and the Class are entitled to actual, consequential, and nominal damages and injunctive relief, with amounts to be determined at trial.

COUNT VII – DECLARTORY JUDGMENT
(On Behalf of Plaintiff and the Class)

175. Plaintiff incorporates by reference all allegations of the preceding paragraphs as though fully set forth herein.

176. Under the Declaratory Judgment Act, 28 U.S.C. § 2201, et seq., this Court is authorized to enter a judgment declaring the rights and legal relations of the parties and grant further necessary relief. Further, the Court has broad authority to restrain acts, such as here, that are tortious and violate the terms of the federal and state statutes described in this Complaint.

177. An actual controversy has arisen in the wake of the Data Breach regarding Plaintiff's and the Class's PII and whether Defendants is currently maintaining data security measures adequate to protect Plaintiff and the Class from further data breaches that compromise their PII. Plaintiff alleges that Defendants' data security measures remain inadequate. Defendants publicly deny these allegations. Furthermore, Plaintiff continues to suffer injury as a result of the

compromise of her PII and remains at imminent risk that further compromises of their PII will occur in the future. It is unknown what specific measures and changes Defendants have undertaken in response to the Data Breach.

178. Plaintiff and the Class have an ongoing, actionable dispute arising out of Defendants' inadequate security measures, including (i) Defendants' failure to encrypt Plaintiff's and the Class's PII, including Social Security numbers, while storing it in an Internet-accessible environment, and (ii) Defendants' failure to delete PII it has no reasonable need to maintain in an Internet-accessible environment, including the Social Security numbers of Plaintiff and the Class.

179. Pursuant to its authority under the Declaratory Judgment Act, this Court should enter a judgment declaring, among other things, the following:

- a. Defendants owe a legal duty to secure the PII of Plaintiff and the Class;
- b. Defendants continue to breach this legal duty by failing to employ reasonable measures to secure consumers' PII; and
- c. Defendants' ongoing breaches of its legal duty continue to cause Plaintiff and the Class harm.

180. This Court also should issue corresponding prospective injunctive relief requiring Defendants to employ adequate security protocols consistent with law and industry and government regulatory standards to protect consumers' PII. Specifically, this injunction should, among other things, direct Defendants to:

- a. engage third party auditors, consistent with industry standards, to test its systems for weakness and upgrade any such weakness found;
- b. audit, test, and train its data security personnel regarding any new or modified procedures and how to respond to a data breach;

- c. regularly test its systems for security vulnerabilities, consistent with industry standards;
- d. implement an education and training program for appropriate employees regarding cybersecurity.

181. If an injunction is not issued, Plaintiff and Class Members will suffer irreparable injury, and lack an adequate legal remedy, in the event of another data breach at Defendants. The risk of another such breach is real, immediate, and substantial. If another breach at Defendants occurs, Plaintiff will not have an adequate remedy at law because many of the resulting injuries are not readily quantified and they will be forced to bring multiple lawsuits to rectify the same conduct.

182. The hardship to Plaintiff and Class Members if an injunction is not issued exceeds the hardship to Defendants if an injunction is issued. Plaintiff will likely be subjected to substantial identity theft and other damage. On the other hand, the cost to Defendants of complying with an injunction by employing reasonable prospective data security measures is relatively minimal, and Defendants have a pre-existing legal obligation to employ such measures.

183. Issuance of the requested injunction will not disserve the public interest. To the contrary, such an injunction would benefit the public by preventing another data breach at Defendants, thus eliminating the additional injuries that would result to Plaintiff and others whose confidential information would be further compromised.

VII. PRAYER FOR RELIEF

WHEREFORE, Plaintiff and the Class pray for judgment against Defendants as follows:

- a. An order certifying this action as a class action under Fed. R. Civ. P. 23, defining the Class as requested herein, appointing the undersigned as Class

counsel, and finding that Plaintiff are a proper representative of the Class requested herein;

- b. A judgment in favor of Plaintiff and the Class awarding them appropriate monetary relief, including actual and statutory damages, punitive damages, attorney fees, expenses, costs, and such other and further relief as is just and proper;
- c. An order providing injunctive and other equitable relief as necessary to protect the interests of the Class and the general public as requested herein, including, but not limited to:
 - i. Ordering that Defendants engage third-party security auditors/penetration testers as well as internal security personnel to conduct testing, including simulated attacks, penetration tests, and audits on Defendants' systems on a periodic basis, and ordering Defendants to promptly correct any problems or issues detected by such third-party security auditors;
 - ii. Ordering that Defendants engage third-party security auditors and internal personnel to run automated security monitoring;
 - iii. Ordering that Defendants audit, test, and train its security personnel regarding any new or modified procedures;
 - iv. Ordering that Defendants segment customer data by, among other things, creating firewalls and access controls so that if one area of Defendants' systems is compromised, hackers cannot gain access to other portions of Defendants' systems;

- v. Ordering that Defendants purge, delete, and destroy in a reasonably secure manner customer data not necessary for their provisions of services;
 - vi. Ordering that Defendants conduct regular database scanning and securing checks; and
 - vii. Ordering that Defendants routinely and continually conduct internal training and education to inform internal security personnel how to identify and contain a breach when it occurs and what to do in response to a breach.
- d. An order requiring Defendants to pay the costs involved in notifying the Class Members about the judgment and administering the claims process;
 - e. A judgment in favor of Plaintiff and the Class awarding them pre-judgment and post-judgment interest, reasonable attorneys' fees, costs and expenses as allowable by law; and
 - f. An award of such other and further relief as this Court may deem just and proper.

VIII. DEMAND FOR JURY TRIAL

Plaintiff demands a trial by jury on all issues so triable.

Dated: February 18, 2025

Respectfully submitted,

By: /s/ Lee A. Floyd

Lee A. Floyd (VSB No. 88459)

Justin M. Sheldon, Esq. (VSB No. 82632)

BREIT BINIAZAN, PC

2100 East Cary Street, Suite 310

Richmond, Virginia 23223

Telephone: (804) 351-9040

Facsimile: (804) 351-9170

Lee@bbtrial.com

Justin@bbtrial.com

William B. Federman*

Jessica A. Wilkes*

Federman & Sherwood

10205 N. Pennsylvania Ave

Oklahoma City, OK 73120

(405) 235-1560

wbf@federmanlaw.com

jaw@federmanlaw.com

Attorneys for Plaintiff

*Admission Pro Hac Vice Forthcoming